UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

SANDRA KUFFREY, individually and on behalf of all others similarly situated, *Plaintiff,* v. COMMUNITY HEALTH SYSTEMS, INC., and CHSPSC, LLC, *Defendants*.	**Case No. _____** **COMPLAINT – CLASS ACTION** **JURY DEMAND**

Plaintiff Sandra Kuffrey ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against defendants Community Health Systems, Inc., and CHSPSC, LLC (collectively, "CHS" or "Defendants"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI"). The PII and PHI may have included names, addresses, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as dates of birth and Social Security numbers.

2. Defendants failed to comply with industry standards to protect information systems that contain PII and PHI, and failed to provide adequate notice to Plaintiff and other Class Members that their PII and PHI had been compromised. Plaintiff seeks, among other things, orders requiring Defendants to fully and accurately disclose the nature of the information that has been

compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. On February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra, LLC ("Fortra"), disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers use "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

4. On or around February 10, 2023, the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT, and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days.

5. On February 13, 2023, defendant Community Health Systems, Inc. reported to the Securities and Exchange Commission ("SEC") that it was one of the customers whom Fortra had notified, that the PII and PHI of "certain patients of the Company's affiliates were exposed by Fortra's attacker," and that CHS estimated that "approximately one million individuals may have been affected by" the incident.

6. On February 22, 2023, the U.S. Department of Health and Human Services' ("HHS") Health Sector Cybersecurity Coordination Center issued a "Sector Alert" emphasizing that Clop's claim referenced its ability to target health care systems.

7. On or around March 8, 2023, CHS posted a notice and began reporting to the attorneys general of certain states additional details regarding the Data Breach in compliance with the laws of those states. However, as of the date of this Complaint, CHS has not yet complied with federal law requiring it to report to the U.S. Department of Health and Human Services' Office for Civil Rights.

8. CHS could have prevented this theft had it limited the customer information it shared with its business associates and employed reasonable measures to ensure its business associates implemented and maintained adequate data security measures and protocols in order to secure and protect CHS patients' data.

9. Plaintiff and Class Members would not have provided their PII and PHI to CHS if they had known that CHS would breach its promises and agreements by failing to ensure that its vendors used adequate security measures, and/or providing its patients' PII and PHI to business associates that utilized inadequate security measures.

10. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and/or PHI were stolen in the Data Breach. Plaintiff seeks remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to CHS's data security policies and practices.

PARTIES

11. Plaintiff Sandra Kuffrey resides in Dayton, Tennessee. Ms. Kuffrey has been a patient at a CHS facility. In a letter dated March 15, 2023, defendant CHSPSC, LLC disclosed to Ms. Kuffrey that her PII and/or PHI was accessible as a result of the Data Breach. Under the heading "What Information Was Involved?," that letter included the following: "The following types of data may have included personal information such as your full name and Social Security number." *See* **Ex. 1**.

12. Defendant Community Health Systems, Inc. is a Delaware corporation, with its principal place of business in Franklin, Tennessee.

13. Defendant CHSPSC, LLC ("CHSPSC") is a Delaware corporation, with its principal place of business in Franklin, Tennessee.

14. CHS refers to itself as "one of the largest hospital organizations in the nation" with 79 hospitals in 16 states, and approximately 66,000 employees. Due to the nature of these the services it provides, CHS acquires and electronically stores patient PII and PHI.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as CHS is a citizen of a state different from that of at least one Class Member.

16. This Court has personal jurisdiction over CHS because it is a resident of the State of Tennessee.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because CHS transacts business and may be found in this District.

FACTUAL ALLEGATIONS

The Data Breach

18. CHS represented in its most recent annual report to the SEC that it "provid[es] a broad range of general and specialized hospital healthcare services and outpatient services to patients in the communities in which [CHS is] located. Those locations include healthcare delivery systems in 46 distinct markets across 16 states [including] 80 affiliated hospitals, with approximately 13,000 beds, and . . . more than 1,000 sites of care, including physician practices,

urgent care centers, freestanding emergency departments, occupational medicine clinics, imaging centers, cancer centers and ambulatory surgery centers." As a healthcare provider, CHS is required to ensure that PII and PHI are not disclosed or disseminated to unauthorized third parties without its patients' express written consent.

19. CHS has long been well-versed as to the threat hackers pose to confidential medical information. On September 23, 2020, HHS reported the following:

> In April 2014, the Federal Bureau of Investigation (FBI) notified CHSPSC that it had traced a cyberhacking group's advanced persistent threat to CHSPSC's information system. Despite this notice, the hackers continued to access and exfiltrate the protected health information (PHI) of 6,121,158 individuals until August 2014. The hackers used compromised administrative credentials to remotely access CHSPSC's information system through its virtual private network.
>
> OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls.

Defendant CHSPSC, LLC agreed to pay $2.3 million to OCR and "adopt a corrective action plan" as a result of that breach.

20. Two weeks later, CHS entered into a multi-state settlement agreement with 28 participating states, providing its payment of $5 million, and adoption information security measures, including:

- development of a written incident response plan;
- incorporation of security awareness and privacy training for all personnel with access to PHI;
- limitation of unnecessary or inappropriate access to PHI; and
- implementation of specific policies and procedures regarding business associates, including use of business associate agreements and *audits of business associates*.

See AG Grewal: NJ Reaches Settlement with Community Health Systems over Data Breach (Oct. 8, 2020), available at https://www.nj.gov/oag/newsreleases20/pr20201008b.html (last accessed Mar. 14, 2023) (emphasis added).

21. Fortra was one of CHS's "business associates." Nevertheless, on February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers use "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

22. On or around February 10, 2023, the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT, and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days.

23. On February 13, 2023, CHS reported to the SEC that it was one of the customers whom Fortra had notified, that the PII and PHI of "certain patients of the Company's affiliates were exposed by Fortra's attacker," and that CHS estimated that "approximately one million individuals may have been affected by" the incident.

24. On March 6, 2023, CHS posted a notice regarding the Data Breach on its website, and purportedly alerted media outlets nationwide. The notice disclosed that the disclosed PII and PHI "may have included full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and social security number." *See* **Ex. 2**.

25. On March 16, 2023, CHS reported to the U.S. Department of Health and Human Services Office for Civil Rights that 962,884 individuals were affected by the Data Breach.

26. CHS's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what CHS knows about the degree to which the data has been disseminated.

27. CHS has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, CHS has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff's and Class Members' interests, and ensure that CHS has proper measures in place to prevent similar incidents from occurring in the future.

CHS's Privacy Policies

28. The Health Insurance Portability and Accountability Act ('HIPAA') requires that CHS maintain strict privacy practices. CHS's Notice of Privacy Practices includes 20 purposes for which CHS might use and disclose patients' medical information. None of those purposes encompass the disclosure of that information to cybercriminals. But the Notice provides that CHS "will first obtain your written authorization before using or disclosing your protected health information for any purpose not described" in the Notice.

29. CHS's Code of Conduct for its personnel provides that they "are expected to protect the privacy of individually identifiable health information and protected health information ('PHI'), in any format, at all times … . All of the facilities within the organization have specific

policies describing patient confidentiality and release of information rules that conform to Applicable Laws governing the release or disclosure of health information."

30. The Code of Conduct further provides that "[p]atient information may only be … released as permitted or required under the Health Insurance Portability and Accountability Act ('HIPAA') or other privacy laws." The CHS personnel responsible for its relationship with Fortra violated the Code of Conduct.

31. In late 2021, CHS issued a Community Impact Report, in which it claimed to "employ an extensive vetting process to review vendor services and solutions before implementation, which includes a security risk assessment. Vendors are assessed for the strength and effectiveness of their security controls, and these requirements are reflected in our contracts and Business Associate Agreements."[1]

The Healthcare Sector is a Primary Target for Data Breaches

32. CHS was on notice that companies in the healthcare industry are susceptible targets for data breaches.

33. CHS was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working

[1] Community Impact Report, at 64 (available at https://www.chs.net/CHS%202020-21%20Community%20Impact%20Report.pdf) (last accessed Mar. 20, 2023).

when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[2]

34. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020[3], to 1,638 in 2021.[4] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[5]

35. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore

[2] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf) (last accessed Mar. 14, 2023).

[3] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Mar. 14, 2023).

[4] *See* Verizon 2022 Data Breach Investigations Report, at 83 (available at https://www.verizon.com/ business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf) (last accessed Mar. 14, 2023).

[5] *Id.* at 62.

[6] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available at https://www.idtheftcenter.org/2018-data-breaches) (last accessed Mar. 14, 2023).

coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[8]

36. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[9] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

37. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

---

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/) (last accessed Mar. 14, 2023).

[8] *Id.*

[9] *2019 HIMSS Cybersecurity Survey* (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last accessed Mar. 14, 2023).

threaten the privacy and security of patients' health and financial information, but also patient access to care.[11]

38. As a major healthcare provider, CHS knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on CHS's patients because of a breach. CHS failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

CHS Stores Plaintiff's and Class Members' PII and PHI

39. CHS obtains and stores a massive amount of its patients' PII and PHI. As a condition of engaging in health services, CHS requires that patients entrust it with highly confidential PII and PHI.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, CHS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

41. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and, as CHS's current and former patients, they rely on CHS to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

42. CHS was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

---

[11] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019) (available at https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last visited Mar. 14, 2023).

43. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[12] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[13]

44. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

45. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

46. The ramifications of CHS's failure to keep its patients' PII and PHI secure are long-lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to

---

[12] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed Mar. 14, 2023).

[13] Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/) (last accessed Mar. 14, 2023).

[14] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at https://khn.org/news/rise-of-indentity-theft/) (last accessed Mar. 14, 2023).

victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

47. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

48. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [15] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[16]

49. Here, not only PHI, but also patient Social Security numbers were compromised. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[17] This time lag between when harm occurs and when it is discovered, and between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

50. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these

---

[15] *See* Medical ID Theft Checklist (available at https://www.identityforce.com/blog/medical-id-theft-checklist-2) (last accessed Mar. 14, 2023).

[16] Experian, The Potential Damages and Consequences of Medical Identityy Theft and Healthcare Data Breaches (available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf) (last accessed Mar. 14, 2023).

[17] *Identity Theft and Your Social Security Number*, Social Security Administration (available at http://www.ssa.gov/pubs/EN-05-10064.pdf) (last accessed Mar. 14, 2023).

fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

51. Changing or cancelling a stolen Social Security number is extremely difficult. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

53. CHS knew, or should have known, the importance of safeguarding its patients' PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on CHS's patients because of a breach. CHS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[18] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015) (available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft) (last visited Mar. 14, 2023).

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

54. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

55. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, CHS's policies and practices with respect to maintaining the security of its patients' PII and PHI were reckless, or at the very least, negligent.

56. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be compensated for the time they have expended because of CHS's misfeasance.

57. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[19]

58. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

[19] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Mar. 14, 2023).

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

CHS's Lax Security Violates HIPAA

59. CHS had a non-delegable duty to ensure that all PHI it collected and stored was secure.

60. CHS is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

61. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information"

which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

62. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

63. HIPAA requires that CHS implement appropriate safeguards for this information.

64. Moreover, HIPAA provides that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as CHS and Fortra. 45 C.F.R. § 164.104.

65. CHS is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity *or business associate* creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306 (emphasis added).

66. Despite these requirements, CHS failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, CHS failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff's and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software

programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

67. CHS failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff's and Class Members' PHI.

CHS Violated FTC Guidelines

68. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited CHS from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' PII is an "unfair practice" in violation of the FTC Act. *See, e.g., Fed. Trade Comm'n v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

69. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

70. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[21] The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

71. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting

[20] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed Mar. 14, 2023).

[21] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

[22] FTC, *Start With Security*, *supra*.

from these actions further clarify the measures businesses must take to meet their data security obligations.

73. CHS failed to properly implement basic data security practices. CHS's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

74. CHS was at all times fully aware of its obligation to protect its patients' PII and PHI because of its position as a healthcare provider. CHS was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

75. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All persons in the United States whose PII and/or PHI was exposed by the Data Breach that was disclosed by CHS on or around February 13, 2023.

76. Excluded from the Class are CHS, any entity in which CHS has a controlling interest, and CHS's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

77. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiff.

78. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. In its report to the SEC, CHS estimated that over one million patients were affected by the Data Breach. All Class Members' names and addresses are available

from CHS's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

79. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. whether and to what extent CHS had a duty to protect the PII and PHI of Class Members;

b. whether CHS was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI;

c. whether CHS had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. whether CHS took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

e. whether CHS failed to adequately safeguard the PII and PHI of Class Members;

f. whether CHS failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. whether CHS adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

h. whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of CHS's wrongful conduct;

i. whether Plaintiff and Class Members are entitled to restitution because of CHS's wrongful conduct;

j. whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

80. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was disclosed by CHS. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through CHS's common misconduct. Plaintiff is advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

81. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against CHS to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

82. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because CHS has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. CHS's policies challenged herein apply to and affect Class Members

uniformly and Plaintiff's challenge of these policies hinges on CHS's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

83. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like CHS. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

84. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because CHS would necessarily gain an unconscionable advantage in non-class litigation, since CHS would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

85. The litigation of Plaintiff's claims is manageable. CHS's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

86. Adequate notice can be given to Class Members directly using information maintained in CHS's records.

87. Unless a class-wide injunction is issued, CHS may continue to maintain inadequate security with respect to the PII and PHI of Class Members, CHS may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and CHS may continue to act unlawfully as set forth in this Complaint.

COUNT I
NEGLIGENCE

88. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

89. As a condition of their utilizing CHS's services, patients were obligated to provide CHS with certain PII and PHI, including their dates of birth, Social Security numbers, personal medical information, and other PII and PHI.

90. Plaintiff and the Class Members entrusted their PII and PHI to CHS on the premise and with the understanding that CHS would safeguard their information and not disclose that information to unauthorized third parties.

91. CHS has full knowledge of the sensitivity of PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if PII and PHI were wrongfully disclosed.

92. CHS knew or reasonably should have known that the failure to exercise due care in the collection, storage, and use of patients' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

93. CHS had a duty to exercise reasonable care in safeguarding, securing, and protecting Plaintiff's and Class Members' PII and PHI from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing CHS's security protocols to ensure that Plaintiff's and Class Members' information in CHS's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained as to proper measures regarding the security of patients' PII and PHI.

94. CHS had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and PHI.

95. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as CHS, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of CHS's duty in this regard.

96. CHS violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and failing to comply with relevant industry standards. CHS's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly considering the growing number of data breaches of healthcare providers.

98. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. CHS knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the importance of providing adequate security for that information, and that CHS had inadequate employee training and education and information technology security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

99. CHS's misconduct created a foreseeable risk of harm to Plaintiff and Class Members. CHS's misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Breach. CHS's misconduct also included its decisions not to comply with industry standards for the safekeeping and disclosure of Plaintiff's and Class Members' PII and PHI.

100. Plaintiff and Class Members had no ability to protect their PII and PHI that was in CHS's possession.

101. CHS was in a position to protect against the harm that Plaintiff and Class Members suffered as a result of the Data Breach.

102. CHS had and continues to have a duty to adequately disclose that Plaintiff's and Class Members' PII and PHI within CHS's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when it was compromised. Such notice was necessary to allow Plaintiff and Class Members to take steps to

prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI by unauthorized parties.

103. CHS has admitted that Plaintiff's and Class Members' PII and PHI was wrongfully disclosed to unauthorized parties because of the Data Breach.

104. CHS, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI during the period in which that information was within CHS's possession or control.

105. CHS failed to heed industry warnings and alerts to provide adequate safeguards to protect patients' PII and PHI in the face of increased risk of theft.

106. CHS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII and PHI.

107. CHS, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

108. But for CHS's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII and PHI would not have been compromised.

109. There is a close causal connection between CHS's failure to implement security measures to protect its patients' PII and PHI and the harm suffered or risk of imminent harm suffered by Plaintiff and Class Members. Unauthorized parties gained access to Plaintiff's and Class Members' PII and PHI as the proximate result of CHS's failure to exercise reasonable care

in safeguarding that information by adopting, implementing, and maintaining appropriate security measures.

110. As a direct and proximate result of CHS's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with the effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remains in CHS's possession and is subject to further unauthorized disclosures so long as CHS fails to undertake appropriate and adequate measures to protect that information; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of CHS's services that Plaintiff and Class Members received.

111. As a direct and proximate result of CHS's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
NEGLIGENCE PER SE

112. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

113. Pursuant to the FTC Act, 15 U.S.C. § 45, CHS had a duty to provide adequate data security practices, including in connection with its sale of its services to Plaintiff's and Class Members' pediatric practices.

114. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, CHS had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

115. CHS breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA, among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of its services, to safeguard Plaintiff's and Class Members' PII/PHI.

116. CHS's failure to comply with applicable laws and regulations constitutes negligence per se.

117. But for CHS's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

118. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of CHS's breach of its duties. CHS knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

119. As a direct and proximate result of CHS's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

120. As a direct and proximate result of CHS's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT

121. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

122. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by CHS and that was stolen in the Data Breach.

123. CHS benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. CHS understood that it so benefitted.

124. CHS also understood and appreciated that Plaintiffs' and Class Members' PHI and PII was private and confidential and that its value depended upon CHS maintaining its privacy and confidentiality.

125. But for CHS's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with CHS. Further, if CHS had disclosed that its data security measures were inadequate, CHS would not have been permitted to continue in operation by regulators and the healthcare marketplace.

126. As a result of CHS's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII), CHS has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

127. CHS's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class

Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

128. Under the common law doctrine of unjust enrichment, it is inequitable for CHS to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PHI and PII in an unfair and unconscionable manner. CHS's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

129. The benefit conferred upon, received, and enjoyed by CHS was not conferred officiously or gratuitously, and it would be inequitable and unjust for CHS to retain the benefit.

COUNT IV
INJUNCTIVE/DECLARATORY RELIEF

130. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

131. CHS owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

132. CHS still stores Plaintiff's and Class Members' PII and PHI.

133. Since the Data Breach, CHS has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

134. CHS has not satisfied its legal duties to Plaintiff and Class Members.

135. Actual harm has arisen in the wake of the Data Breach regarding CHS's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class

Members are at risk of additional or further harm due to the exposure of their PII and PHI, and CHS's failure to address the security failings that led to that exposure.

136. Plaintiff, therefore, seeks a declaration: (a) that CHS's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, CHS must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that CHS engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on CHS's systems on a periodic basis, and ordering CHS to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that CHS engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that CHS audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that CHS segment patient data by, among other things, creating firewalls and access controls so that if one area of CHS's system is compromised, hackers cannot gain access to other portions of CHS's systems;

e. ordering that CHS purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provision of services;

f. ordering that CHS conduct regular computer system scanning and security checks;

g. ordering that CHS routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering CHS to meaningfully educate its current, former, and prospective patients about the threats they face because of the loss of their PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiff and [his/her] counsel to represent the Class;

b. for equitable relief enjoining CHS from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling CHS to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: March 28, 2023

Respectfully submitted,

HERZFELD, SUETHOLZ, GASTEL, LENISKI AND WALL, PLLC

By: */s/ Benjamin A. Gastel*
Benjamin A. Gastel (BPR #28699)
The Freedom Center
223 Rosa L. Parks Avenue, Suite 300
Nashville, Tennessee 37203
(615) 800-6225
ben@hsglawgroup.com

BAILEY GLASSER LLP
Bart D. Cohen (*pro hac vice* application forthcoming)
1622 Locust Street
Philadelphia, PA 19103
(215) 274-9420
bcohen@baileyglasser.com

Attorneys for Plaintiff and the Proposed Class